

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	§	Group Art Unit: 2614
Michael W. Brown, <i>et al.</i>	§	
	§	Examiner: Patel, Hemant Shantilal
Serial No.: 10/645,959	§	
	§	Atty Docket No.: AUS920010819US2
Filed: 08/22/2003	§	
	§	Customer No.: 34533
Title: Intermediary Device Initiated	§	
Caller Identification	§	Confirmation No.: 8404

**Mail Stop: Appeal Brief-Patents**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

**APPEAL BRIEF**

**Honorable Commissioner:**

This is an Appeal Brief filed pursuant to 37 CFR § 41.37 in response to the Office Action of April 27, 2007 (hereinafter the “Office Action”), and pursuant to the Notice of Appeal filed July 27, 2007.

**REAL PARTY IN INTEREST**

The real party in interest in accordance with 37 CFR § 41.37(c)(1)(i) is the patent assignee, International Business Machines Corporation (“IBM”), a New York corporation having a place of business at Armonk, New York 10504.

## **RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences within the meaning of 37 CFR §41.37(c)(1)(ii).

## **STATUS OF CLAIMS**

Status of claims in accordance with 37 CFR § 41.37(c)(1)(iii): Thirty-two (32) claims are filed in the original application in this case. Claims 1-32 are rejected in the Office Action. Claims 1-32 are on appeal.

## **STATUS OF AMENDMENTS**

Status of amendments in accordance with 37 CFR § 41.37(c)(1)(iv): No amendments were submitted after final rejection. The claims as currently presented are included in the Appendix of Claims that accompanies this Appeal Brief.

## **SUMMARY OF CLAIMED SUBJECT MATTER**

Appellants provide the following concise summary of the claimed subject matter according to 37 CFR § 41.37(c)(1)(v). This summary includes a concise explanation of the subject matter defined in each of the independent claims involved in the appeal and includes references to the specification by page and line number and to the drawings by reference characters. The eight independent claims involved in this appeal are claims 1, 7, 12, 13, 19, 25, 31, and 32. Claim 1 is a method claim. Claims 7 and 12 recite counterpart aspects of the method of claim 1. Claim 7 recites system aspects of the method of claim 1, and claim 12 recites computer program product aspects of the method of claim 1. Claim 13 is also a method claim. Claims 19 and 25 recite counterpart aspects of the method of claim 13. Claim 19 recites system aspects of the method of claim 13, and claim 25 recites computer program product aspects of the method of claim 13. Claims 31 and 32 are independent method claims.

Claim 1 recites a method for specifying telephone services for a particular caller (page 14, lines 3-9). The method of claim 1 includes detecting a call initiation condition from an origin device at a trusted telephone network (page 18, lines 19-26). The method of claim 1 also includes brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The method of claim 1 also includes, responsive to receiving from said external server, an authenticated caller identity of a caller utilizing said origin device, specifying services available to said caller according to said authenticated caller identity (page 16, lines 10-15).

Claim 7 recites a system for specifying telephone services for a particular caller (page 14, lines 3-9). The system of claim 7 includes a trusted telephone network for providing service to an origin telephony device (page 13, lines 16-19, Figure 1 at reference characters 10 and 11a-11n). The system of claim 7 includes means for detecting a call initiation condition from said origin telephony device at said trusted telephone network (page 18, lines 19-26). The system of claim 7 also includes means for brokering a connection between said origin device and a server external to said trusted telephone network to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The system of claim 7 also includes means responsive to receiving an authenticated caller identity of a caller utilizing said origin telephony device from said server, for specifying services available to said caller according to said authenticated caller identity (page 16, lines 10-15).

Claim 12 recites a computer program product for specifying telephone services for a particular caller (page 14, lines 3-9). The computer program product of claim 12 includes a recording medium (page 28, lines 15-25). The computer program product of claim 12 also includes means, recorded on said recording medium, for detecting a call initiation condition from an origin telephony device at a trusted telephone network (page 18, lines 19-26). The computer program product of claim 12 also includes means, recorded on said recording medium, for brokering a connection between said origin device and a

server external to said trusted telephone network to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The computer program product of claim 12 also includes means, recorded on said recording medium, for specifying services available to said caller according to an authenticated caller identity received from said server to identify a caller utilizing said origin telephony device (page 16, lines 10-15).

Claim 13 recites a method for informing a callee of a caller identity (page 14, lines 20-26). The method of claim 13 includes detecting a call initiation condition from an origin device at a trusted telephone network (page 18, lines 19-26). The method of claim 13 also includes brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The method of claim 13 also includes responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller identity to a destination device, such that a callee receiving said call at said destination device is provided with an identity of a party originating said call (page 21, lines 7-11, and Figure 2 at reference characters 42 and 44).

Claim 19 recites a system for informing a callee of a caller identity (page 14, lines 20-26). The system of claim 19 includes a trusted telephone network for enabling telephone service (page 13, lines 16-19, Figure 1 at reference characters 10 and 11a-11n). The system of claim 19 also includes means for detecting a call initiation condition from an origin device at said trusted telephone network (page 18, lines 19-26). The system of claim 19 also includes means for brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The system of claim 19 also includes means responsive to receiving an authenticated caller identity of a caller utilizing said origin device from said external server, for transferring said authenticated caller identity to a destination device to identify said caller to a call (page 21, lines 7-11, and Figure 2 at reference characters 42 and 44).

Claim 25 recites a computer program product for informing a callee of a caller identity (page 14, lines 20-26). The computer program product of claim 25 includes a recording medium (page 28, lines 15-25). The computer program product of claim 25 also includes means, recorded on the recording medium, for detecting a call initiation condition from an origin device at a trusted telephone network (page 18, lines 19-26). The computer program product of claim 25 also includes means, recorded on the recording medium, for brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service (page 15, lines 11-15; Figure 1, reference character 22). The computer program product of claim 25 also includes means, recorded on the recording medium, for transferring an authenticated caller identity received from said external server to a destination device to identify said caller utilizing said origin device (page 21, lines 7-11, and Figure 2 at reference characters 42 and 44).

Claim 31 recites a method for controlling caller identification (page 15, lines 11-21, and page 21, lines 7-11). The method of claim 31 includes receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone network initiates said authentication service (page 15, lines 11-21). The method of claim 31 also includes controlling output of said authenticated caller identity from said telephony device, such that an individual with access to said telephony device is informed of the identity of said caller (page 21, lines 7-11).

Claim 32 recites a method for controlling a call (page 27, line 3 – page 28, line 9). The method of claim 32 includes receiving, at a telephony device, a secure communication channel via a trusted telephone network to an authentication service provided by an external server, wherein said trusted telephone network initiates said authentication service (page 27, lines 4-9). The method of claim 32 also recites facilitating, from said telephony device, communications between said authentication service and a caller, such that said authentication service is enabled to authenticate an identity of said caller (page 27, line 17 – page 28, line 9).

## GROUND OF REJECTION

In accordance with 37 CFR § 41.37(c)(1)(vi), Appellants provide the following concise statement for each ground of rejection:

1. Claims 1-14, 17-20, 23-26, and 29-32 are rejected under 35 U.S.C. § 102(b) over Farris, *et al.* (U.S. Patent No. 6,122,357).
2. Claims 15-16, 21-22, and 27-28 stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Farris in view of Rozenblit (U.S. Patent No. 5,832,072).

## ARGUMENT

Appellants present the following arguments pursuant to 37 CFR § 41.37(c)(1)(vii) regarding the two grounds of rejection in the present case.

**Argument Regarding The First Ground Of Rejection On Appeal:  
Claims 1-14, 17-20, 23-26, and 29-32 Are Rejected Under  
35 U.S.C. § 102(b) As Being Unpatentable Over Farris**

Claims 1-14, 17-20, 23-26, and 31-32 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Farris. To anticipate claims 1-14, 17-20, 23-26, and 31-32 under 35 U.S.C. § 102(b), Farris must disclose each and every element and limitation recited in the claims of the present application. As explained below, Farris does not disclose each and every element and limitation recited in the claims of the present application and therefore does not anticipate claims of the present application.

**Farris Does Not Disclose Each and Every Element  
Of The Claims Of The Present Application**

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). As explained in more detail below, Farris does not disclose each and every element of claims 1, 13, 31, or 32, and Farris therefore cannot be said to anticipate the claims of the present application within the meaning of 35 USC § 102(b).

**Farris Does Not Disclose Each and Every Element  
Of Claim 1 Of The Present Application**

As explained in detail below, Farris does not disclose each and every element and limitation recited in claim 1 of the present application and therefore does not anticipate claim 1 of the present application. Independent claim 1 recites:

A method for specifying telephone services for a particular caller,  
comprising:

detecting a call initiation condition from an origin device at a trusted  
telephone network;

brokering a connection between said origin device and an external server  
enabled to perform a caller identity authentication service; and

responsive to receiving, from said external server, an authenticated caller  
identity of a caller utilizing said origin device, specifying services  
available to said caller according to said authenticated caller identity.

**Farris Does Not Disclose Brokering A Connection Between  
Said Origin Device And An External Server Enabled To  
Perform A Caller Identity Authentication Service**

The Office Action takes the position that Farris at column 18, line 22 – column 19, line 5, discloses the second element of claim 1: brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service. Appellants respectfully note in response, however, that what Farris at column 18, line 22 – column 19, line 5, in fact discloses is:

In response to the off-hook and the off-hook trigger set in the subscriber's profile, the SSP type central office switch 11.sub.1 launches a query to the SCP 19 (step S3). Specifically, the SSP 11.sub.1 creates a TCAP query message containing relevant information, such as the office equipment (OE) number assigned to the off-hook line, and transmits that query over an SS7 link to one of the STPs 15. The query includes a destination point code and/or a global title translation addressing the message to the SCP 19, and the STP 15 relays the query message over the appropriate link to the SCP 19. The query from the SSP central office 11.sub.1 identifies the caller's line by its associated office equipment (OE) number and possibly by a single telephone number associated with the off-hook line.

In response to a query, the SCP 19 accesses its a database, typically, the MSAP database set up in the ISCP, to determine how to process the particular call. The SCP 19 identifies an access key in the query and uses the key to retrieve the appropriate record from the database. In this case, the query indicates an off-hook trigger as the trigger event, therefore the SCP 19 uses the calling party office equipment (OE) number as the access key. The SCP 19 retrieves a call processing record (CPR) corresponding to the office equipment (OE) number associated with the off-hook line and proceeds in accord with that CPR (step S4).

For the present example of the personal dial tone service, the CPR will provide information necessary for routing the call to some node of the network that will perform speaker identification/verification (SIV). In the preferred embodiment, the SIV is a function performed by an Intelligent Peripheral (IP), therefore the CPR provides information for routing the call to the nearest available IP having the SIV capability.

Based on the CPR, the SCP 19 formulates a response message instructing the SSP central office 11.sub.1 serving the customer to route the call. In this case, the message includes information, e.g. a office equipment (OE) number or telephone number, used for routing a call to the identified IP 23.



The SCP 19 formulates a TCAP message in SS7 format, with the destination point code identifying the SSP office 11.sub.1. The SCP 19 transmits the TCAP response message back over the SS7 link to the STP 15, and the STP 15 in turn routes the TCAP message to the SSP central office 11.sub.1 (see step S5)

The SSP type switch in the central office 11.sub.1 uses the routing information to connect the call to one of the lines or channels to the IP 23. A two-way voice grade call connection now extends between the calling station 1.sub.A and the IP 23 (step S6) . In the present example, the switch actually connects the off-hook line to the line to the IP before providing dial tone.

That is, Farris at column 18, line 22 – column 19, line 5, discloses a CPR (call processing record) that provides information necessary for routing a call to some node of the network that will perform speaker identification/verification. Farris's CPR that provides information necessary for routing a call to some node of the network that will perform speaker identification/verification does not disclose brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service as claimed in the present application. Farris does not disclose here, or at any other reference point, 'an external server enabled to perform a caller identity authentication service' as claimed in the present application. In fact, at this reference point, Farris teaches away from Appellants' claimed invention by teaching "routing the call to some node *of the network* that will perform speaker identification/verification." Farris' routing a call to some node of the network teaches directly away from *an external server* enabled to perform a caller identity authentication service as claimed in the present application. Because Farris does not disclose each and every element and limitation of Appellants' claims, Farris does not anticipate Appellants' claims, and the rejections under 35 USC § 102(b) should be withdrawn.

In the Office Action's Response to Arguments on page 2 of the Office Action, the Office Action states:

... Farris' IP providing speech verification is external to the central office of a trusted telephone network (PSTN) and the central office brokers connection between the caller and this external IP (Farris, col. 18, ll. 22 –

col. 20, ll. 49). As shown in Farris Figs. 1, 3, this independent IP is connected to the trusted network (PSTN) thru Integrated Services Digital Network (ISDN) links as well as data network (Internet) with TCP/IP. It was known in the art, that customer premises equipments (CPE), i.e. third party servers providing special services, connected to telephone service provider network (PSTN) using Primary Rate Interface (PRI) of ISDN. These CPEs were not part of the PSTN owned and operated by telephone service provider but they were some external server nodes on the network and were accessible to any other subscriber on the PSTN. Thus, the IP connected to PSTN is an external server node connected on the network.

That is, the Office Action takes the position that Farris' Intelligent Peripheral ('IP') that provides speech verification is external to the central office of Farris' trusted telephone network ('PSTN') because is connected to Farris' PSTN through Integrated Services Digital Network ('ISDN') links, and it was well known in the art that customer premises equipment ('CPE') that connected to a PSTN through Primary Rate Interface ('PRI') of ISDN were not part of the PSTN. Appellants respectfully note in response, however, that "customer premises equipments (CPE), i.e. third party servers providing special services, connected to telephone service provider network (PSTN) using Primary Rate Interface (PRI) of ISDN" is not available to the Examiner in this case as Well Known Prior Art.

According to MPEP § 2144.03, the Examiner may use as Well Known Prior Art facts outside the record only if such facts are capable of instant and unquestionable demonstration as being well-known in the art. Well Known Prior Art, however, may not be substituted for facts which cannot be instantly and unquestionably demonstrated. As indicated in *In re Lee*, the examiner's finding of whether there is a disclosure in the reference must not be resolved based on "subjective belief and unknown authority," but must be "based on objective evidence of record." *In re Lee*, 277 F.3d 1338, 1343-44, 61 USPQ2d 1430, 1433-34 (Fed. Cir. 2002). The court in *Lee* requires evidence for the determination of unpatentability by clarifying that "common knowledge and common sense," as mentioned in *In re Bozek*, 416 F.2d 1385, 1390, 163 USPQ 545, 549 (CCPA 1969), may only be applied to analysis of the evidence, rather than be a substitute for evidence. *In re Lee*, 277 F.3d at 1345, 61 USPQ2D at 1435.

In this case, Appellants note with respect that the Examiner has made a mere naked assertion that a fact is well known in the prior art with absolutely no “objective evidence of record.” As mentioned, Well Known Prior Art may not be substituted for facts which cannot be instantly and unquestionably demonstrated. The assertion in the Office Action that it was well known in the prior art that “customer premises equipments (CPE), i.e. third party servers providing special services, connected to telephone service provider network (PSTN) using Primary Rate Interface (PRI) of ISDN” cannot be instantly and unquestionably demonstrated. In fact such assertion is directly contradicted in Farris because Farris defines the PSTN as including one or more IPs. *See* Farris column 11, lines 1-4. The Office Action therefore cannot rely on such assertion to support that Farris’ IP is disclosed in the Well Known Prior Art as an external node to the PSTN. For these reasons, the rejection based on well know prior art fails to disclose brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service as claimed in the present application. Not disclosing each and every limitation of Appellants’ claims, Farris does not anticipate Appellants’ claims, and the rejections under 35 U.S.C. § 102(b) should be withdrawn.

**Farris Does Not Disclose Responsive To Receiving, From  
Said External Server, An Authenticated Caller Identity  
Of A Caller Utilizing Said Origin Device, Specifying  
Services Available To Said Caller According To  
Said Authenticated Caller Identity**

The Office Action takes the position that Farris at column 20, lines 6-49, discloses the third element of claim 1: responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, specifying services available to said caller according to said authenticated caller identity. Appellants respectfully note in response, however, that what Farris at column 20, lines 6-49, in fact discloses is:

In step S13, the IP 23 determines if the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber (within some threshold level of certainty). If there is a match, the IP now knows the identity of the calling subscriber. Based

on the identification of the calling subscriber, the IP 23 selects a virtual office equipment (OE) number from storage that corresponds to the subscriber.

The IP 23 formulates a D-channel signaling message containing the virtual office equipment (OE) number together with an instruction to load that OE number into the register assigned to the call in place of the OE number of the off-hook line. The IP 23 supplies the message to the SSP central office switch 11.sub.1 over the D-channel of the ISDN PRI link (step S14). In response, the administrative module processor 61 rewrites the OE number in the register assigned to the call using the OE number received from the IP 23.

Upon rewriting the OE number in the register, the administrative module processor 61 of central office switch 11.sub.1 also reloads the profile information in the register (step S15). Specifically, the administrative module processor 61 retrieves profile information associated with the virtual office equipment (OE) number from the disc storage 63 into the register. As such, the profile information in the assigned register in the call store 67 now corresponds to the identified subscriber, rather than to the off-hook line.

The profile information provides a wide range of data relating to the subscriber's services. The profile data provides necessary billing information, enabling billing from the call to this particular subscriber. The profile also defines various service features available to this subscriber on outgoing calls, such as three-way calling. The profile may define a class of calling service available to the subscriber. In the dormitory example, the caller may be allowed a set dollar amount for long distance calls per month (e.g. \$50.00). The profile data will indicate the remaining amount at the time of the call and will cause the switch to interrupt service when the available amount is exhausted. Other class of service restrictions might enable long distance calls only if collect and/or only if calling one or two specified numbers (e.g. only to the parent's house). The class of service might enable only long distance calls within a region or country but not international calls.

That is, Farris at column 20, lines 6-49, discloses an administrative module processor that retrieves profile information associated with a virtual office equipment number. Farris's administrative module processor that retrieves profile information associated with a virtual office equipment number does not disclose responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, specifying services available to said caller according to said authenticated caller identity

as claimed in the present application. As explained above, Farris does not disclose an *external server*, as claimed in the present application, but instead teaches at column 18, lines 57-55, an intelligent peripheral as a “node of the network that will perform speaker identification/verification,” that is, a node of the *same* network. Because Farris does not disclose an external server as claimed here, Farris cannot be said to disclose, responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, specifying services available to said caller according to said authenticated caller identity as claimed in the present application. Because Farris does not disclose each and every element and limitation of Appellants’ claims, Farris does not anticipate Appellants’ claims, and the rejections under 35 USC § 102(b) should be withdrawn.

**Farris Does Not Disclose Each and Every Element  
Of Claim 13 Of The Present Application**

As explained in detail below, Farris does not disclose each and every element and limitation recited in claim 13 of the present application and therefore does not anticipate claim 13 of the present application. Independent claim 13 recites:

A method for informing a callee of a caller identity, comprising:

detecting a call initiation condition from an origin device at a trusted telephone network;

brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service; and

responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller identity to a destination device, such that a callee receiving said call at said destination device is provided with an identity of a party originating said call.

**Farris Does Not Disclose Brokering A Connection Between  
Said Origin Device And An External Server Enabled To  
Perform A Caller Identity Authentication Service**

The Office Action takes the position that Farris at column 18, line 22 – column 19, line 5, discloses the second element of claim 13: brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service. Farris at column 18, line 22 – column 19, line 5, quoted above, discloses a CPR (call processing record) that provides information necessary for routing a call to some node of the network that will perform speaker identification/verification. Farris’s CPR that provides information necessary for routing a call to some node of the network that will perform speaker identification/verification does not disclose brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service as claimed in the present application. Farris does not disclose here, or at any other reference point, ‘an external server enabled to perform a caller identity authentication service’ as claimed in the present application. In fact, at this reference point, Farris teaches away from Appellants’ claimed invention by teaching “routing the call to some node *of the network* that will perform speaker identification/verification.” Farris’s “node of the network” clearly refers to a node of the *same* network, teaching away from *an external server* enabled to perform a caller identity authentication service as claimed in the present application. Because Farris does not disclose each and every element and limitation of Appellants’ claims, Farris does not anticipate Appellants’ claims, and the rejections under 35 USC § 102(b) should be withdrawn.

**Farris Does Not Disclose Responsive To Receiving, From  
Said External Server, An Authenticated Caller Identity Of A Caller  
Utilizing Said Origin Device, Transferring Said Authenticated  
Caller Identity To A Destination Device, Such That A Callee  
Receiving Said Call At Said Destination Device Is Provided  
With An Identity Of A Party Originating Said Call**

The Office Action takes the position that Farris at column 20, lines 6-32, and column 21, line 53- column 22, line 18, discloses the third element of claim 13: responsive to

receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller identity to a destination device, such that a callee receiving said call at said destination device is provided with an identity of a party originating said call. Appellants respectfully noted in response to the Previous Office Action, however, that what Farris at column 20, lines 6-32, in fact discloses is:

In step S13, the IP 23 determines if the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber (within some threshold level of certainty). If there is a match, the IP now knows the identity of the calling subscriber. Based on the identification of the calling subscriber, the IP 23 selects a virtual office equipment (OE) number from storage that corresponds to the subscriber.

The IP 23 formulates a D-channel signaling message containing the virtual office equipment (OE) number together with an instruction to load that OE number into the register assigned to the call in place of the OE number of the off-hook line. The IP 23 supplies the message to the SSP central office switch 11.sub.1 over the D-channel of the ISDN PRI link (step S14). In response, the administrative module processor 61 rewrites the OE number in the register assigned to the call using the OE number received from the IP 23.

Upon rewriting the OE number in the register, the administrative module processor 61 of central office switch 11.sub.1 also reloads the profile information in the register (step S15). Specifically, the administrative module processor 61 retrieves profile information associated with the virtual office equipment (OE) number from the disc storage 63 into the register. As such, the profile information in the assigned register in the call store 67 now corresponds to the identified subscriber, rather than to the off-hook line.

In addition, what Farris at column 21, line 53- column 22, line 18, in fact discloses is:

When the terminating office 11.sub.N receives the IAM message, the administrative module processor for that office retrieves the customer profile for the number in the destination number field of that message (e.g. the number for the telephone 1.sub.B) from its mass storage system and loads that profile into one of its call store registers. If the called party has an enhanced caller ID service, with name display, the terminating central office 11.sub.N would normally recognize the attempt to complete to that party's number message as a terminating attempt trigger (TAT) type point

in call (PIC) to trigger access to the LIDB database for name information. However, in this embodiment of the invention, the terminating end office detects the receipt of the subscriber's name data with the IAM message, therefore the administrative module processor in that office overrides the trigger.

The terminating central office switching system 11.sub.N transmits an Address Complete Message (ACM) back to the central office 11.sub.1 and if the called line is available applies ringing signal to the called party's line (S182). The ACM includes a variety of information, including a calling party status indicator, e.g. line free or busy. If the line is not busy, the end office 13 rings the station Y corresponding to the dialed digits 703-333-5678, and generates the appropriate indicator in the Address Complete Message (ACM) to indicate that it received the request for a call and that the number is not busy. The ACM message is sent back by simply reversing the point codes from the IAM message. Now the destination point code (DPC) is the point code of the central office 11, and the origination point code (OPC) is the point code of the central office 13. In response to the ACM message, if the called line is available, the originating central office 11 applies a ringback tone signal to the line to the calling station 1.sub.A (S183).

That is, Farris at these reference points discloses the administrative module processor retrieves profile information associated with the virtual office equipment number. Farris's administrative module processor that retrieves profile information associated with the virtual office equipment number does not disclose responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller identity to a destination device, such that a callee receiving said call at said destination device is provided with an identity of a party originating said call. Farris does not disclose at this reference point or any other, an external server as claimed in the present application, but instead teaches at column 18, lines 57-55, an intelligent peripheral as a "node of the network that will perform speaker identification/verification." Again, Farris's "node of the network," clearly referring to a node of the *same* network, cannot be said to teach an *external* server as claimed here. Because Farris does not disclose an external server as claimed here Farris cannot be said to disclose, responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller identity to a destination device, such that a callee receiving said call at said destination



device is provided with an identity of a party originating said call as claimed in the present application. Because Farris does not disclose each and every element and limitation of Appellants' claims, Farris does not anticipate Appellants' claims, and the rejections under 35 USC § 102(b) should be withdrawn.

**Farris Does Not Disclose Each and Every Element  
Of Claim 31 Of The Present Application**

As explained in detail below, Farris does not disclose each and every element and limitation recited in claim 31 of the present application and therefore does not anticipate claim 31 of the present application. Independent claim 31 recites:

A method for controlling caller identification, comprising:

receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone network initiates said authentication service; and

controlling output of said authenticated caller identity from said telephony device, such that an individual with access to said telephony device is informed of the identity of said caller.

**Farris Does Not Disclose Receiving, From A Trusted Telephone Network, An Authenticated Caller Identity For A Caller At A Telephony Device, Wherein Said Caller Identity Is Authenticated At A Authentication Service Accessible Via A Network External To Said Trusted Telephone Network, Wherein Said Trusted Telephone Network Initiates Said Authentication Service**

The Office Action takes the position that Farris at column 18, line 48 – column 20, line 23, discloses the first element of claim 31: receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone network initiates said authentication service. Appellants respectfully noted in response to the Previous Office Action, however, that what Farris at column 18, line 48 – column 20, line 23, in fact discloses is:

For the present example of the personal dial tone service, the CPR will provide information necessary for routing the call to some node of the network that will perform speaker identification/verification (SIV). In the preferred embodiment, the SIV is a function performed by an Intelligent Peripheral (IP), therefore the CPR provides information for routing the call to the nearest available IP having the SIV capability.

Based on the CPR, the SCP 19 formulates a response message instructing the SSP central office 11.sub.1 serving the customer to route the call. In this case, the message includes information, e.g. a office equipment (OE) number or telephone number, used for routing a call to the identified IP 23. The SCP 19 formulates a TCAP message in SS7 format, with the destination point code identifying the SSP office 11.sub.1. The SCP 19 transmits the TCAP response message back over the SS7 link to the STP 15, and the STP 15 in turn routes the TCAP message to the SSP central office 11.sub.1 (see step S5)

The SSP type switch in the central office 11.sub.1 uses the routing information to connect the call to one of the lines or channels to the IP 23. A two-way voice grade call connection now extends between the calling station 1.sub.A and the IP 23 (step S6) . In the present example, the switch actually connects the off-hook line to the line to the IP before providing dial tone.

As noted above, the communication link to the IP 23 provides both line connections and signaling, preferably over a primary rate interface (PRI) type ISDN link. When the central office 11.sub.1 extends the call from the calling party's line to a line circuit (over a B channel) to the IP 23, the switch in that office also provides call related data over the signaling link (D channel for ISDN). The call related data, for example, includes the office equipment (OE) number normally associated with the off-hook line and possibly the telephone number for that line.

In response to the incoming call, the IP 23 will seize the line, and it will launch its own query to the SCP 19 (step S7). In the preferred network illustrated in FIG. 1, the IP 23 and the SCP 19 communicate with each other via a separate second signalling network 27, for example utilizing either an 1129+ protocol or a generic data interface (GDI) protocol as discussed in U.S. Pat. No. 5,572,583 to Wheeler, Jr. et al. The query from the IP 23 again identifies the caller's line by at least its associated office equipment (OE) number.

In response to the query from the IP 23, the SCP 19 again accesses the appropriate CPR (step S8) and provides a responsive instruction back through the network 27 to the IP 23 (step S9). Although the IP 23 could passively monitor any speech that the user might utter, the preferred implementation utilizes a 'Challenge Phase' to prompt the user to input specific identifying information. In this case, the instruction causes the IP 23 to provide a prompt message over the connection to the caller (step S10). Here, the signal to the caller may be a standard dial tone or any other appropriate audio signal. Preferably, the instruction from the SCP 19 causes the IP 23 to provide an audio announcement prompting the caller to speak personal information. In one preferred example, in step S10 the IP plays an audio prompt message asking the caller, 'Please say your full name'. The process may ask for any appropriate identifying information.

The signal received by the IP 23 goes over the lines and through the central office switch(es) for presentation via the off-hook telephone 1.sub.A to the calling party. In response, the caller will speak identifying information into their off-hook telephone, and the network will transport the audio signal to the IP 23 (step S11).

As noted above, an IP 23 can provide a wide range of call processing functions, such as message playback and digit collection. In the preferred system, the IP also performs speaker identification/verification (SIV) on the audio signal received from the off-hook telephone in step S11. When the IP 23 receives speech input information during actual call processing, for this service example, the IP analyzes the speech to extract certain characteristic information (step S12).

The IP 23 stores a template or other voice pattern information for each person who has the personalized service in the area that the IP normally services. If the IP 23 does not store the particular template or feature information it needs to process a call, the IP 23 can communicate with a remote IP 23.sub.R to obtain that information. In the present shared line example, the IP 23 will store template or feature data for each subscriber associated with the particular off-hook line.

When the IP 23 receives input speech and extracts the characteristic information during actual call processing, the IP compares the extracted speech information to stored pattern information, to identify and authenticate the particular caller. In the present example, the voice authentication module 233 in the IP 23 compares the extracted speech information to the stored template or feature data for each subscriber associated with the particular off-hook line.

In step S13, the IP 23 determines if the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber (within some threshold level of certainty). If there is a match, the IP now knows the identity of the calling subscriber. Based on the identification of the calling subscriber, the IP 23 selects a virtual office equipment (OE) number from storage that corresponds to the subscriber.

The IP 23 formulates a D-channel signaling message containing the virtual office equipment (OE) number together with an instruction to load that OE number into the register assigned to the call in place of the OE number of the off-hook line. The IP 23 supplies the message to the SSP central office switch 11.sub.1 over the D-channel of the ISDN PRI link (step S14). In response, the administrative module processor 61 rewrites the OE number in the register assigned to the call using the OE number received from the IP 23.

That is, Farris at column 18, line 48 – column 20, line 23, discloses routing a call to the identified Intelligent Peripheral (IP) that determines whether the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber. Farris's routing of a call to the identified IP that determines whether the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber does not disclose receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone

network initiates said authentication service. As explained above, Farris does not disclose “an authentication service accessible via a network external to said trusted telephone network” as claimed here. In fact, Farris’s authentication is taught as occurring in the intelligent peripheral which is a node of Farris’s network. Because Farris does not disclose “an authentication service accessible via a network external to said trusted telephone network,” it cannot be said that Farris discloses receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone network initiates said authentication service as claimed here. Because Farris does not disclose each and every element and limitation of Appellants’ claims, Farris does not anticipate Appellants’ claims, and the rejections under 35 USC § 102(b) should be withdrawn

**Farris Does Not Disclose Each and Every Element  
Of Claim 32 Of The Present Application**

As explained in detail below, Farris does not disclose each and every element and limitation recited in claim 32 of the present application and therefore does not anticipate claim 32 of the present application. Independent claim 32 recites:

A method for controlling a call, comprising:

receiving, at a telephony device, a secure communication channel via a trusted telephone network to an authentication service provided by an external server, wherein said trusted telephone network initiates said authentication service; and

facilitating, from said telephony device, communications between said authentication service and a caller, such that said authentication service is enabled to authenticate an identity of said caller.

**Farris Does Not Disclose Receiving, At A Telephony  
Device, A Secure Communication Channel Via A Trusted  
Telephone Network To An Authentication Service Provided  
By An External Server, Wherein Said Trusted Telephone  
Network Initiates Said Authentication Service**

The Office Action takes the position that Farris at column 18, line 48 – column 19, line 24 and column 20, lines 6-23, discloses the first element of claim 32: receiving, at a telephony device, a secure communication channel via a trusted telephone network to an authentication service provided by an external server, wherein said trusted telephone network initiates said authentication service. Appellants respectfully note in response, however, that what Farris at column 18, line 48 – column 19, line 24, in fact discloses is:

For the present example of the personal dial tone service, the CPR will provide information necessary for routing the call to some node of the network that will perform speaker identification/verification (SIV). In the preferred embodiment, the SIV is a function performed by an Intelligent Peripheral (IP), therefore the CPR provides information for routing the call to the nearest available IP having the SIV capability.

Based on the CPR, the SCP 19 formulates a response message instructing the SSP central office 11.sub.1 serving the customer to route the call. In this case, the message includes information, e.g. a office equipment (OE) number or telephone number, used for routing a call to the identified IP 23. The SCP 19 formulates a TCAP message in SS7 format, with the destination point code identifying the SSP office 11.sub.1. The SCP 19 transmits the TCAP response message back over the SS7 link to the STP 15, and the STP 15 in turn routes the TCAP message to the SSP central office 11.sub.1 (see step S5)

The SSP type switch in the central office 11.sub.1 uses the routing information to connect the call to one of the lines or channels to the IP 23. A two-way voice grade call connection now extends between the calling station 1.sub.A and the IP 23 (step S6) . In the present example, the switch actually connects the off-hook line to the line to the IP before providing dial tone.

As noted above, the communication link to the IP 23 provides both line connections and signaling, preferably over a primary rate interface (PRI) type ISDN link. When the central office 11.sub.1 extends the call from the calling party's line to a line circuit (over a B channel) to the IP 23, the switch in that office also provides call related data over the signaling link

(D channel for ISDN). The call related data, for example, includes the office equipment (OE) number normally associated with the off-hook line and possibly the telephone number for that line.

In response to the incoming call, the IP 23 will seize the line, and it will launch its own query to the SCP 19 (step S7). In the preferred network illustrated in FIG. 1, the IP 23 and the SCP 19 communicate with each other via a separate second signalling network 27, for example utilizing either an 1129+ protocol or a generic data interface (GDI) protocol as discussed in U.S. Pat. No. 5,572,583 to Wheeler, Jr. et al. The query from the IP 23 again identifies the caller's line by at least its associated office equipment (OE) number.

In addition, what Farris at column 20, lines 6-23, actually discloses is:

In step S13, the IP 23 determines if the information extracted from the speech input matches any of the stored template data feature data for an identifiable subscriber (within some threshold level of certainty). If there is a match, the IP now knows the identity of the calling subscriber. Based on the identification of the calling subscriber, the IP 23 selects a virtual office equipment (OE) number from storage that corresponds to the subscriber.

The IP 23 formulates a D-channel signaling message containing the virtual office equipment (OE) number together with an instruction to load that OE number into the register assigned to the call in place of the OE number of the off-hook line. The IP 23 supplies the message to the SSP central office switch 11.sub.1 over the D-channel of the ISDN PRI link (step S14). In response, the administrative module processor 61 rewrites the OE number in the register assigned to the call using the OE number received from the IP 23.

That is, what Farris discloses at these reference points is that the CPR will provide information necessary for routing the call to some node of the network that will perform speaker identification/verification. Farris's CPR that will provide information necessary for routing the call to some node of the network that will perform speaker identification/verification does not disclose receiving, at a telephony device, a secure communication channel via a trusted telephone network to an authentication service provided by an external server, wherein said trusted telephone network initiates said authentication service as claimed in the present application. Farris, as explained in detail

above, does not disclose an external server that provides authentication services. Because Farris does not disclose each and every element and limitation of Appellants' claims, Farris does not anticipate Appellants' claims, and the rejections under 35 USC § 102(b) should be withdrawn.

### **Farris Does Not Enable Each and Every Element Of The Independent Claims Of The Present Application**

Not only must Farris disclose each and every element of the claims of the present application within the meaning of *Verdegaal* in order to anticipate Appellants' claims, but also Farris must be an enabling disclosure of each and every element of the claims of the present application within the meaning of *In re Hoeksema*. In *Hoeksema*, the claims were rejected because an earlier patent disclosed a structural similarity to the Appellant's chemical compound. The court in *Hoeksema* stated: "We think it is sound law, consistent with the public policy underlying our patent law, that before any publication can amount to a statutory bar to the grant of a patent, its disclosure must be such that a skilled artisan could take its teachings in combination with his own knowledge of the particular art and be in possession of the invention." *In re Hoeksema*, 399 F.2d 269, 273, 158 USPQ 596, 600 (CCPA 1968). The meaning of *Hoeksema* for the present case is that unless Farris places Appellants' claims in the possession of a person of ordinary skill in the art, Farris is legally insufficient to anticipate Appellants' claims under 35 U.S.C. § 102(b). As explained above, Farris does not disclose each and every element and limitation of the independent claims 1, 13, 31, and 32 of the present application. Because Farris does not disclose each and every element and limitation of the independent claims, Farris cannot possibly place the elements and limitations of the independent claims 1, 13, 31, and 32 in the possession of a person of ordinary skill in the art. Farris cannot, therefore, anticipate claims 1, 13, 31, and 32 of the present application.

### **Relations Among Claims**

Independent claim 1 claims method aspects of specifying telephone services for a particular caller according to embodiments of the present invention. Independent claims



7 and 12 respectively claim system and computer program product aspects of specifying telephone services for a particular caller according to embodiments of the present application. For the same reason that Farris does not disclose or enable a method for specifying telephone services for a particular caller, therefore, Farris also does not disclose or enable either a system or a computer program product for specifying telephone services for a particular caller corresponding to independent claims 7 and 12. Independent claims 7 and 12 are therefore patentable and should be allowed.

Independent claim 13 claims method aspects of informing a callee of a caller identity according to embodiments of the present invention. Independent claims 19 and 25 respectively claim system and computer program product aspects of informing a callee of a caller identity according to embodiments of the present application. For the same reason that Farris does not disclose or enable a method for informing a callee of a caller identity, therefore, Farris also does not disclose or enable either a system or a computer program product for informing a callee of a caller identity corresponding to independent claims 19 and 25. Independent claims 19 and 25 are therefore patentable and should be allowed.

Claims 2-6, 8-11, 14-18, 20-24, and 26-30 depend respectively from independent claims 1, 7, 13, 19, and 25. Each dependent claim includes all of the limitations of the independent claim from which it depends. Because Farris does not disclose or enable each and every element of the independent claims, Farris does not disclose or enable each and every element of the dependent claims of the present application. As such, claims 2-6, 8-11, 14-18, 20-24, and 26-30 are also patentable and should be allowed.

**Argument Regarding The Second Ground Of Rejection On Appeal:  
Claims 15-16, 21-22, And 27-28 Are Rejected Under 35 U.S.C. § 103(a)  
As Being Unpatentable Over Farris In View Of Rozenblit**

Claims 15-16, 21-22, and 27-28 stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Farris in view of Rozenblit. The question of whether Appellants claims are obvious *vel non* is examined in light of: (1) the scope and content

of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int'l Co. v. Teleflex Inc.*, No. 04-1350, slip op. at 2 (U.S. April 30, 2007). Although Appellants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Appellants' claims for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of the references must teach or suggest all of Appellants' claim limitations. *Manual of Patent Examining Procedure* § 2142 (citing *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974)). Dependent claims 15-16, 21-22, and 27-28, depend from independent claims 13, 19, and 25, and include all the limitations of the independent claims from which they depend. In rejecting dependent claims 15-16, 21-22, and 27-28, the Office Action relies on Farris as disclosing each and every element of independent claims 13, 19, and 25. As Appellants have demonstrated above, Farris in fact does not disclose each and every element of independent claims 13, 19, and 25. Because the proposed combination of Farris and Rozenblit relies on the argument that Farris discloses each and every element of claims 13, 19, and 25 and because Farris in fact does not disclose each and every element of claims 13, 19, and 25, the proposed combination of Farris and Rozenblit cannot teach or suggest all the claim limitations of dependent claims 15-16, 21-22, and 27-28. The proposed combination of Farris and Rozenblit, therefore, cannot establish a prima facie case of obviousness, and the rejections should be withdrawn.

#### **CONCLUSION OF APPELLANTS' ARGUMENTS**


Claims 1-14, 17-20, 23-26, and 31-32 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Farris. Farris does not disclose or enable each and every element of Appellants' claims. Farris therefore does not anticipate Appellants' claims. Claims 1-14, 17-20, 23-26, and 31-32 are therefore patentable and should be allowed. Appellants respectfully request reconsideration of claims 1-14, 17-20, 23-26, and 31-32.

Claims 15-16, 21-22, and 27-28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Farris in view of Rozenblit. The combination of Farris and Rozenblit does not teach or suggest each and every element of Appellants' claims. Claims 15-16, 21-22, and 27-28 are therefore patentable and should be allowed. Appellants respectfully request reconsideration of claims 15-16, 21-22, and 27-28.

In view of the forgoing arguments, reversal on all grounds of rejection is requested.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0447 for any fees required or overpaid.

Date: September 25, 2007

Respectfully submitted,  
By:   
John Biggers  
Reg. No. 44,537  
Biggers & Ohanian, LLP  
P.O. Box 1469  
Austin, Texas 78767-1469  
Tel. (512) 472-9881  
Fax (512) 472-9887  
ATTORNEY FOR APPELLANTS

**APPENDIX OF CLAIMS  
ON APPEAL IN PATENT APPLICATION OF  
MICHAEL WAYNE BROWN, *ET AL.*, SERIAL NO. 10/645,959**

CLAIMS

What is claimed is:

1. A method for specifying telephone services for a particular caller, comprising:  
  
detecting a call initiation condition from an origin device at a trusted telephone network;  
  
brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service; and  
  
responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, specifying services available to said caller according to said authenticated caller identity.
2. The method for specifying telephone services according to claim 1, wherein said server is accessible via a network outside said trusted telephone network.
3. The method for specifying telephone services according to claim 1, further comprising:  
  
retrieving a caller profile for said authenticated caller identity; and  
  
specifying a selection of services from among a plurality of services that are offered for said call according to said caller profile.

4. The method for specifying telephone services according to claim 1, wherein said authenticated caller identity is authenticated by a voice utterance of said caller.

5. The method for specifying telephone services according to claim 1, wherein brokering a connection further comprises:

transmitting a request for said caller identity authentication service via a signal gateway to a network for accessing said external server;

transferring a prompt for a voice utterance, received from said external server via a media gateway, to said origin device;

transferring a voice utterance by said caller through said media gateway to said network for accessing said external server; and

receiving said authenticated caller identity via said signal gateway at said trusted telephone network.

6. The method for specifying telephone services according to claim 1, wherein brokering a connection further comprises:

brokering a secure connection between said trusted telephone network and said external server.

7. A system for specifying telephone services for a particular caller, comprising:

a trusted telephone network for providing service to an origin telephony device;

means for detecting a call initiation condition from said origin telephony device at said trusted telephone network;

means for brokering a connection between said origin device and a server external to said trusted telephone network to perform a caller identity authentication service; and

means responsive to receiving an authenticated caller identity of a caller utilizing said origin telephony device from said server, for specifying services available to said caller according to said authenticated caller identity.

8. The system for specifying telephone services according to claim 7, wherein said server is accessible via a network external to trusted telephone network.
9. The system for specifying telephone services according to claim 7, further comprising:

means for retrieving a caller profile for said authenticated caller identity; and

means for specifying a selection of services from among a plurality of services that are offered for said call according to said caller profile.

10. The system for specifying telephone services according to claim 7, wherein said authenticated caller identity is authenticated by a voice utterance of said caller.
11. The system for specifying telephone services according to claim 7, wherein said means for brokering a connection further comprises:

means for transmitting a request for said caller identity authentication service via a signal gateway to a network for accessing said server;

means for transferring a prompt for a voice utterance, received from said server via a media gateway, to said origin device;

means for transferring a voice utterance by said caller through said media gateway to said network for accessing said server; and

means for receiving said authenticated caller identity via said signal gateway at said trusted telephone network.

12. A computer program product for specifying telephone services for a particular caller, comprising:

a recording medium;

means, recorded on said recording medium, for detecting a call initiation condition from an origin telephony device at a trusted telephone network;

means, recorded on said recording medium, for brokering a connection between said origin device and a server external to said trusted telephone network to perform a caller identity authentication service; and

means, recorded on said recording medium, for specifying services available to said caller according to an authenticated caller identity received from said server to identify a caller utilizing said origin telephony device.

13. A method for informing a callee of a caller identity, comprising:

detecting a call initiation condition from an origin device at a trusted telephone network;

brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service; and

responsive to receiving, from said external server, an authenticated caller identity of a caller utilizing said origin device, transferring said authenticated caller

identity to a destination device, such that a callee receiving said call at said destination device is provided with an identity of a party originating said call.

14. The method for informing a callee of a caller identity according to claim 13, further comprising:

filtering content of said authenticated caller identity before transfer to said destination device.

15. The method for informing a callee of a caller identity according to claim 14, further comprising:

filtering content of said authenticated caller identity according to filtering preferences associated with said authenticated caller identity.

16. The method for informing a callee of a caller identity according to claim 14, further comprising:

filtering content of said authenticated caller identity according to an identity of said callee.

17. The method for informing a callee of a caller identity according to claim 14, further comprising:

filtering said authenticated caller identity to block at least a portion of the content of said authenticated caller identity.

18. The method for informing a caller of a callee identity according to claim 13, further comprising:



responsive to said authenticated caller identity indicating a lack of identity, automatically initiating recording of said call.

19. A system for informing a callee of a caller identity, comprising:

a trusted telephone network for enabling telephone service;

means for detecting a call initiation condition from an origin device at said trusted telephone network;

means for brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service; and

means responsive to receiving an authenticated caller identity of a caller utilizing said origin device from said external server, for transferring said authenticated caller identity to a destination device to identify said caller to a call.

20. The system for informing a callee of a caller identity according to claim 19, further comprising:

means for filtering content of said authenticated caller identity before transfer to said destination device.

21. The system for informing a callee of a caller identity according to claim 20, further comprising:

means for filtering content of said authenticated caller identity according to filtering preferences associated with said authenticated caller identity.

22. The system for informing a callee of a caller identity according to claim 20, further comprising:

means for filtering content of said authenticated caller identity according to an identity of said callee.

23. The system for informing a callee of a caller identity according to claim 20, further comprising:

means for filtering said authenticated caller identity to block at least a portion of the content of said authenticated caller identity.

24. The system for informing a caller of a callee identity according to claim 19, further comprising:

means responsive to said authenticated caller identity indicating a lack of identity, for automatically initiating recording of said call.

25. A computer program product for informing a callee of a caller identity, comprising:

a recording medium;

means, recorded on said recording medium, for detecting a call initiation condition from an origin device at a trusted telephone network;

means, recorded on said recording medium, for brokering a connection between said origin device and an external server enabled to perform a caller identity authentication service; and

means, recorded on said recording medium, for transferring an authenticated caller identity received from said external server to a destination device to identify said caller utilizing said origin device.

26. The computer program product for informing a callee of a caller identity according to claim 25, further comprising:
- means, recorded on said recording medium, for filtering content of said authenticated caller identity before transfer to said destination device.
27. The computer program product for informing a callee of a caller identity according to claim 26, further comprising:
- means, recorded on said recording medium, for filtering content of said authenticated caller identity according to filtering preferences associated with said authenticated caller identity.
28. The computer program product for informing a callee of a caller identity according to claim 26, further comprising:
- means, recorded on said recording medium, for filtering content of said authenticated caller identity according to an identity of said callee.
29. The computer program product for informing a callee of a caller identity according to claim 26, further comprising:
- means, recorded on said recording medium, for filtering said authenticated caller identity to block at least a portion of the content of said authenticated caller identity.
30. The computer program product for informing a caller of a callee identity according to claim 25, further comprising:

means, recorded on said recording medium, for automatically initiating recording of said call when said authenticated caller identity indicates a lack of identity.

31. A method for controlling caller identification, comprising:

receiving, from a trusted telephone network, an authenticated caller identity for a caller at a telephony device, wherein said caller identity is authenticated at a authentication service accessible via a network external to said trusted telephone network, wherein said trusted telephone network initiates said authentication service; and

controlling output of said authenticated caller identity from said telephony device, such that an individual with access to said telephony device is informed of the identity of said caller.

32. A method for controlling a call, comprising:

receiving, at a telephony device, a secure communication channel via a trusted telephone network to an authentication service provided by an external server, wherein said trusted telephone network initiates said authentication service; and

facilitating, from said telephony device, communications between said authentication service and a caller, such that said authentication service is enabled to authenticate an identity of said caller.

**APPENDIX OF EVIDENCE  
ON APPEAL IN PATENT APPLICATION OF  
MICHAEL WAYNE BROWN, *ET AL.*, SERIAL NO. 10,645,959**

This is an evidence appendix in accordance with 37 CFR § 41.37(c)(1)(ix).

There is in this case no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132, nor is there in this case any other evidence entered by the examiner and relied upon by the appellants.

**RELATED PROCEEDINGS APPENDIX**

This is a related proceedings appendix in accordance with 37 CFR § 41.37(c)(1)(x).  
There are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR § 41.37(c)(1)(ii).